Experimental randomness certification with a symmetric informationally complete positive operator-valued measurement

Chenxi Liu (刘晨曦)[1,2,†], Kun Liu (刘 琨)[1,2,†], Xiaorun Wang (汪小润)[1,2], Luyan Wu (吴陆颜)[1,2], Jian Li (李 剑)[1,2,*], and Qin Wang (王 琴)[1,2,]**

[1]*Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

[2]*Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

**Corresponding author: jianli@njupt.edu.cn; **corresponding author: qinw@njupt.edu.cn*

Received March 15, 2020; accepted June 28, 2020; posted online August 28, 2020

Nonlocal correlations observed from entangled quantum particles imply the existence of intrinsic randomness. Normally, locally projective measurements performed on a two-qubit entangled state can only certify one-bit randomness at most, while non-projective measurement can certify more randomness with the same quantum resources. In this Letter, we carry out an experimental investigation on quantum randomness certification through a symmetric informationally complete positive operator-valued measurement, which in principle can certify the maximum randomness through an entangled qubit. We observe the quantum nonlocal correlations that are close to the theoretical values. In the future, this work can provide a valuable reference for the research on the limit of randomness certification.

Keywords: nonlocality; randomness; SIC-POVM.
doi: 10.3788/COL202018.102701.

Quantum correlations are incompatible with any local determinacy[1–4], and they can be used to certify intrinsic randomness in device-independent ways, i.e., implementing measurement on quantum entangled particles. Up to date, the relationship between nonlocality and quantum randomness has been explored by many groups, such as device-independent quantum randomness number generator (DI-QRNG)[5,6], device-independent quantum randomness amplification[7,8], and device-independent quantum key distribution[9,10]. For DI-QRNGs, the observed nonlocal correlations guarantee the randomness of the generated measurement outcomes, and the amount of quantum randomness can be quantified through the violation of different Bell inequalities, e.g., Clauser–Horne–Shimony–Holt (CHSH) inequality[11,12], the chained Bell inequality[13], and Mermin inequality[14,15].

In order to give security proofs for a device-independent randomness generation protocol, the normal way is to assume that an additional observer exists, hereafter called Eve, who has partial access to the quantum state and possesses the ability to predict the measurement outcomes under the framework of quantum mechanics. Denote P_g as the upper bound of the guessing probability, i.e., Eve can correctly predict the measurement results. The value of P_g can be calculated through either numerical derivation methods or by solving optimization problems. In a CHSH experiment introduced in Ref. [5], the local guessing probability $P_g(a, a|\bar{x}, E)$, which means Eve knows one of Alice's (A) measurement outcomes a, bounded by

$$P_g(a, a|\bar{x}, E) \leq \frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{I^2}{4}} \tag{1}$$

in terms of the CHSH inequality I,

$$I = E_{1,2} + E_{1,2} + E_{2,1} - E_{2,2}. \tag{2}$$

$E_{x,y}$ is the expectation value of the product of outcomes when Alice and Bob perform the measurement setting x and y individually. When the measurement bases are selected properly, the maximum quantum violation of CHSH inequality can reach $2\sqrt{2}$. Therefore, the upper bound of the guessing probability is 1/2, indicating that only one-bit randomness is certified in a device-independent way. Beyond the CHSH scenario, Bell experiments based on non-projective measurements have shown some merits to generate more than one-bit randomness. Recently, Andersson *et al.* proved that a symmetric informationally complete positive operator-valued measurement (SIC-POVM) can be used for the certification of two random bits at most[16]. This scheme can be seen as the optimal randomness certification from a two-qubit maximally entangled state.

Here, we report an experimental implementation of randomness certification based on SIC-POVM. Firstly, we experimentally observe the violation of Gisin's elegant Bell inequality (EBI) with a value of 6.8021 ± 0.0825 through a non-collinear type-II beam-like spontaneous parametric down-conversion (SPDC) source[17,18]. Secondly, we use the linear optical system (five-step quantum walks) to implement an SIC-POVM[19,20]. In our experiment, SIC-POVM is certified in a device-independent way. Our experimental results show that the probabilities of the four outcomes of SIC-POVM are closest to the theoretical predictions. The average error of those probabilities is about 0.0057. In the future, we can use the semi-definite programming (SDP)[21] method in the Navascués–Pironio–Acín (NPA) hierarchy[22] to calculate the amount of randomness from the observed quantum correlations. Therefore, our present work can provide a valuable reference for randomness certification with SIC-POVM.

The schematic diagram of standard Bell experiments is shown in Fig. 1. In this system, Alice, Bob, and Eve share a tripartite quantum state $|\Psi_{\mathrm{ABE}}\rangle$ on a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ of arbitrary dimensions. Then Alice and Bob each locally chooses a measurement setting (x or y) and obtains a corresponding measurement outcome (a or b). The aim of Eve is to be able to guess one or more of the outcomes from Alice's or Bob's measurement results. In this case, the joint correlations are summarized by a conditional probability,

$$P(a,b|x,y)=\left\langle \Psi_{\mathrm{ABE}}|M^A_{a|x}\otimes M^B_{b|y}\otimes M^E_e|\Psi_{\mathrm{ABE}}\right\rangle, \tag{3}$$

where $M^A_{a|x}$ denotes the measurement operator associated with the measurement outcome a when Alice performs the measurement setting x, and, similarly, we define Bob's and Eve's measurement operators $M^B_{b|y}$ and M^E_e, respectively. The local guessing probability associated with Eve's guess is consistent with Alice's outcome a,

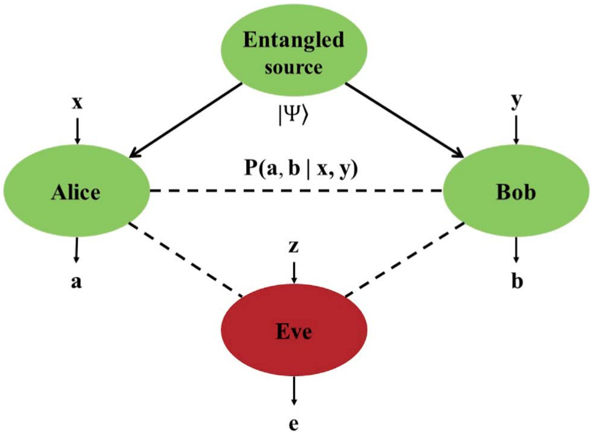

Fig. 1. Standard randomness certification scenario in device-independent ways. An entangled source, two measurement stations, Alice and Bob, and an additional observer, Eve. The source simultaneously emits particles to two measurement stations, Alice and Bob. Each of them randomly performs the local measurement setting x or y and obtains outcome a or b, respectively. The observed correlation is represented by the conditional probability $P(a,b|x,y)$. From the perspective of security, we will assume that Eve might be able to guess the outcomes of Alice's/Bob's measurement.

$$P_g(a,a|\bar{x},E)=\max_Q\sum_a\left\langle \Psi_{\mathrm{ABE}}|M^A_{a|x}\otimes M^B_{b|y}\otimes M^E_e|\Psi_{\mathrm{ABE}}\right\rangle, \tag{4}$$

where Q is all possible quantum realizations, described by quantum state $|\Psi_{\mathrm{ABE}}\rangle$ as well as measurements $M^A_{a|x}$, $M^B_{b|y}$, and M^E_e, and compatible with the observed quantum correlations $P(a,b|x,y)$. The randomness of measurement outcomes can be quantified by the min-entropy $H_{\min}=-\log_2[P_g(a,a|\bar{x},E)]$, which is a function of local guessing probability.

Here, we study the randomness certification based on an EBI and an SIC-POVM. In this scheme, Alice performs three projective measurement settings ($x=1, 2, 3$) and a four-outcome POVM ($x=4$), and Bob performs four projective measurement settings ($y=1, 2, 3, 4$). The EBI is defined as

$$\begin{aligned}S={}&E_{1,1}+E_{1,2}-E_{1,3}-E_{1,4}+E_{2,1}-E_{2,2}+E_{2,3}\\&-E_{2,4}+E_{3,1}-E_{3,2}-E_{3,3}+E_{3,4}\le 6.\end{aligned} \tag{5}$$

The maximum quantum violation of EBI is $S=4\sqrt{3}$, approximately equal to 6.9282. The local guessing probability of Eve is

$$G=\max_E\sum_a P_g(a,a|x=4,E), \tag{6}$$

where $P_g(a,a|x=4,E)$ is the probability that Eve makes a correct guess in consideration of Alice's measurements A_4 and Eve's measurements E. By maximizing all four-outcome POVMs, the local guessing probability G can reach 1/4; then, two-bit randomness can be certified. According to the proof in Ref. [16], the measurement A_4 should be an extremal four-outcome SIC-POVM whose elements correspond to the four linearly independent unit rank projectors:

$$\begin{aligned}A_{1|4}&=\frac{1}{4}\left[I-\frac{1}{\sqrt{3}}(Z+X+Y)\right],\\A_{2|4}&=\frac{1}{4}\left[I-\frac{1}{\sqrt{3}}(Z-X+Y)\right],\\A_{3|4}&=\frac{1}{4}\left[I+\frac{1}{\sqrt{3}}(Z-X+Y)\right],\\A_{4|4}&=\frac{1}{4}\left[I+\frac{1}{\sqrt{3}}(Z+X-Y)\right],\end{aligned} \tag{7}$$

where X, Y, Z are Pauli operators, and I is the identity matrix. The elements of A_4 are anti-aligned with the four projective measurements on Bob's side, and thus all probabilities $P(a=i, b=+1|x=4, y=i)$ are zero. Combined with the maximum violation of EBI, this scheme can certify two-bit randomness. Below we report the experimental verification of this scheme through a linear optical system.

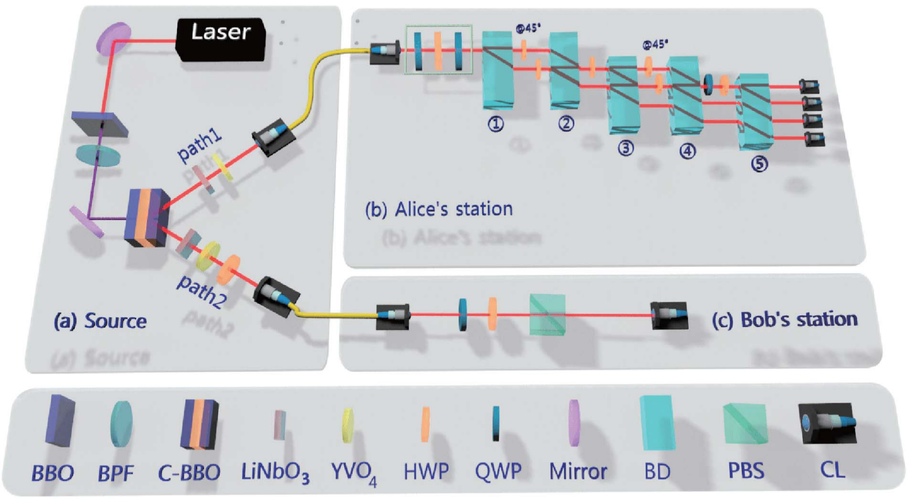

Fig. 2. Schematic of our experimental setup for randomness certification based on SIC-POVM. (a) A maximally entangled state $|\Psi_{\rm AB}\rangle = (|\rm HH\rangle - |\rm VV\rangle)/\sqrt{2}$ is generated with type-II SPDC sources pumped by pulsed lasers. (b) A four-outcome POVM is implemented by employing five-step quantum walks. (c) Projective measurement is implemented with a QWP, an HWP, and a PBS. BBO, β-barium borate crystal; BPF, band pass filter; C-BBO, sandwich-type BBO + HWP + BBO combination; QWP, quarter-wave plate; HWP, half-wave plate; PBS, polarizing beam-splitter; LiNbO$_3$, lithium niobate crystal, which is used for spatial compensation; YVO$_4$, yttrium orthovanadate crystal, which is used for temporal compensation; BD, beam displayer; CL, collimation lens.

As shown in Fig. 2, our experimental setup mainly consists of three parts, the preparation of the maximally entangled state, the non-projective measurement device in Alice's side, and the projective measurement device in Bob's side. Firstly, in order to obtain higher visibility, a non-collinear type-II beam-like SPDC source is used to generate maximally entangled state $|\Psi_{\rm AB}\rangle = (|HH\rangle - |VV\rangle)/\sqrt{2}$, where H and V denote horizontal and vertical polarization, respectively. A mode-locked Ti:sapphire pulsed laser with a pulse duration time of 100 fs and a central wavelength of 780 nm is frequency-doubled into ultraviolet pulses at 390 nm by a β-barium borate (BBO) crystal cut for collinear type-I phase-matching. Then, the resulting 390 nm laser is pumped on a sandwich-type BBO crystal and generates the SPDC photon pairs. After the SPDC process, a pair of LiNbO$_3$ crystals is used for spatial compensation, and a pair of YVO$_4$ crystals is used for temporal compensation. Accordingly, the down-conversion photon pairs from the sandwich-type BBO crystal are indistinguishable both spatially and temporally, and the polarization maximally entangled state $|\Psi_{\rm AB}\rangle$ is generated.

These photon pairs go through interference filters (IFs, Semrock) with a 2 nm bandwidth and a central wavelength at 780 nm and are then coupled into single-mode fibers (SMFs) through a collimation lens (CL, Thorlabs). The photons are then individually sent to Alice's and Bob's measurement stations via SMFs. In the experimental setup, two pairs of beam displacers (BDs) (BD$_1$ and BD$_2$, BD$_3$ and BD$_4$) form an interferometer with a visibility of 99.5% within 12 h. High visibility indicates good parallelism of the optical axis between the two BDs. To perform the non-projective measurement, five-step quantum walks are composed to realize the SIC-POVM [see Fig. 1(b)]. The four elements of SIC-POVM in Ref. [19], named the initial SIC-POVM, are $\Pi_i = \frac{1}{2}(|\psi_4^i\rangle\langle\psi_4^i|)$ $(i = 1, 2, 3, 4)$, where

$$\begin{aligned}
|\psi_4^1\rangle &= |H\rangle,\\
|\psi_4^2\rangle &= -\sqrt{\frac{1}{3}}|H\rangle + \sqrt{\frac{2}{3}}|V\rangle,\\
|\psi_4^3\rangle &= -\sqrt{\frac{1}{3}}|H\rangle + e^{i\frac{2}{3}\pi}\sqrt{\frac{2}{3}}|V\rangle,\\
|\psi_4^4\rangle &= -\sqrt{\frac{1}{3}}|H\rangle + e^{-i\frac{2}{3}\pi}\sqrt{\frac{2}{3}}|V\rangle.
\end{aligned} \tag{8}$$

In order to realize the SIC-POVM defined in Eq. (8), called the target SIC-POVM, we use a set of unitary transformations realized with the sequential placement of quarter-wave plate (QWP$_1$), half-wave plate (HWP$_1$), and QWP$_2$. Through numerical simulations, we obtain the angles of wave-plates for the setting $x = 4$, e.g., $\theta_{Q1} = -2.5°$, $\theta_{H1} = -45°$, $\theta_{Q2} = 17.5°$, $\theta_{H2} = 67.5°$, $\theta_{H3} = 67.5°$, $\theta_{H4} = 17.5°$, $\theta_{Q3} = -37.5°$, and $\theta_{H5} = 60°$. The Bloch vectors of the initial and target SIC-POVMs are shown in Fig. 3. To implement projective measurements, HWP$_2$ and HWP$_4$ are set to 45°, and others (excluding QWP$_3$ and HWP$_5$) are set to 0°. The combination of QWP$_3$, HWP$_5$, and BD$_5$ can be used for projective measurements, and their angles are determined by the specific measurement setting of x $(x = 1, 2, 3)$. This setup can switch the measurements between projective and non-projective measurements by rotating the angles of internal

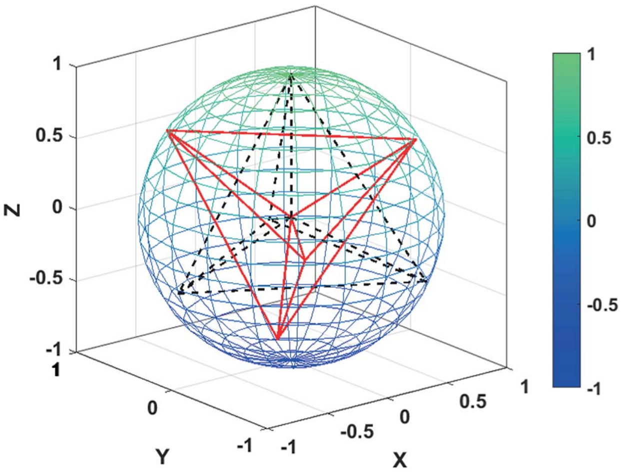

Fig. 3. Bloch vector of SIC-POVM. The tetrahedron formed by the dotted black line represents the initial SIC-POVM, and the tetrahedron formed by the solid red line represents the target SIC-POVM.

Table 1. Theoretical and Experimental Results of the Elegant Bell Inequality

Expectation $E_{x,y}$	Theory	Experiment
$E_{1,1}$	0.5774	0.5637(±0.0076)
$E_{1,2}$	0.5774	0.6047(±0.0063)
$E_{1,3}$	−0.5774	−0.5443(±0.0070)
$E_{1,4}$	−0.5774	−0.5674(±0.0071)
$E_{2,1}$	0.5774	0.4962(±0.0067)
$E_{2,2}$	−0.5774	−0.5091(±0.0068)
$E_{2,3}$	0.5774	0.6314(±0.0070)
$E_{2,4}$	−0.5774	−0.6219(±0.0069)
$E_{3,1}$	0.5774	0.6510(±0.0067)
$E_{3,2}$	−0.5774	−0.5960(±0.0071)
$E_{3,3}$	−0.5774	−0.5125(±0.0065)
$E_{3,4}$	0.5774	0.5155(±0.0069)

wave-plates, which are mounted on electrically controlled rotation stages with high precision.

In Bob's station, the projective measurement is made up of the QWP, HWP, and polarizing beam splitter (PBS) in sequence. The measurements of the setting $y = 1$, 2, 3, 4 are projective measurements with two measurement outcomes +1 and −1. Photons in either Alice's or Bob's station are performed with corresponding measurements and then coupled into SMFs. Finally, they are detected by the single-photon avalanche photodiodes (APDs, Excelitas Technologies) with the typical photon detection efficiency of about 63% at 780 nm. The detection results are recorded by the high-resolution coincidence field-programmable gate array electronics (Timetag, UQDevice).

During the data acquisition phase, a laser with a power of 19 mW is applied. In order to reduce background noises, we set the coincidence count windows at 1 ns, which also results in a decreased accidental coincidence probability. The obtained two-photon coincidence counting rate is about 500 per second, and the recording period is set at 300 s. To be noted, the measurement data should be corrected with the detection efficiencies of utilized APDs. We perform the standard-state tomography process and reconstruct the density matrix (see Fig. 4), getting the state fidelity of 98.3% ± 0.7% compared with the maximally entangled states.

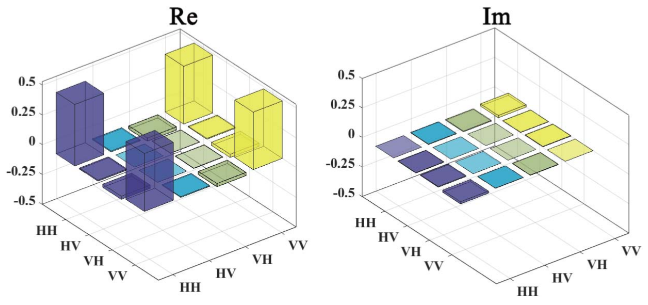

Fig. 4. Tomography of the prepared maximally entangled state. The real and imaginary parts are shown in the left and right panels, respectively.

After executing a total of 48 two-photon projective measurements on the generated entangled states, we can calculate the value for the EBI, $S_{\text{exp}} = 6.8021 \pm 0.0825$. The results of the EBI are listed out in Table 1. The experimental results are calculated with the photon counts through the quantum-state tomography process. The slight discrepancy between each experimental value and the corresponding theoretical result is attributed to the production of the non-ideal maximally entangled state. The violation of the EBI indicates how much randomness can be certified from the experimental data. We calculate that the local guessing probability is 0.6179 based on the violation of EBI, and 0.6946 bits of randomness can be certified. Using the complete nonlocal correlations $P(a, b|x, y)$ ($x \in \{1, 2, 3\}$ and $y \in \{1, 2, 3, 4\}$)[20], the value of the local guessing probability will increase a little. To obtain an upper bound of randomness, we introduce the SIC-POVM in Alice's side ($x = 4$). The probabilities of the four outcomes of SIC-POVM in device-independent certification are shown in Table 2. From the table, we

Table 2. Theoretical and Experimental Values for the Probabilities of the Four Outcomes of SIC-POVM

$P(a = i, b = +1\|x = 4, y = i)$	Theory	Experiment
$P(1, +1\|4, 1)$	0	0.0037
$P(2, +1\|4, 2)$	0	0.0040
$P(3, +1\|4, 3)$	0	0.0081
$P(4, +1\|4, 4)$	0	0.0070
Sum	0	0.0228

can see that the experimental results are closest to the theoretical predictions, and the sum of $P(a=i,\ b=+1|x=4,\ y=i)$ is 0.0228. In the future, we can use the SDP method in the NPA hierarchy[22,23] implemented in the Python package Ncpol2spda to calculate the randomness with all of the observed correlations $P(a,b|x,y)\,(x\in\{1,2,3,4\}$ and $y\in\{1,2,3,4\})$. The numerical analysis on the relationship between randomness and noise sensitivity can be obtained in Ref. [24]. To be noted, the obtained randomness will be lower than two bits due to the randomness certification scheme based on SIC-POVM being sensitive to noise.

In summary, we have carried out experimental randomness certification with an SIC-POVM, and this method can obtain more than one-bit randomness from one entangled qubit. Some works have shown that non-projective measurements have more advantages than projective measurements in randomness certifications. Therefore, our present work can provide valuable references for future design and implementation of randomness certification and random number generators based on SIC-POVM. In the future, our goal is to minimize experimental errors to make a more accurate system and give a specific amount of randomness. In addition, another challenging task is to verify the correlations without loopholes.

This work was financially supported by the National Key R&D Program of China (Nos. 2018YFA0306400 and 2017YFA0304100), the National Natural Science Foundation of China (Nos. 11774180 and 61590932), the Leading-edge Technology Program of Jiangsu Natural Science Foundation (No. BK20192001), and the Postgraduate Research and Practice Innovation Program of Jiangsu Province (No. KYCX18_0915).

[†]These authors contributed equally to this work.

References

1. J. S. Bell, Physics **1**, 195 (1964).
2. N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
3. X. M. Hu, B. H. Liu, Y. Guo, G. Y. Xiang, Y. F. Huang, C. F. Li, and A. Cabello, Phys. Rev. Lett. **120**, 180402 (2018).
4. J. S. Xu, X. Y. Xu, C. F. Li, C. J. Zhang, X. B. Zou, and G. C. Guo, Nat. Commun. **1**, 7 (2010).
5. S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, and C. Monroe, Nature **464**, 1021 (2010).
6. Y. Liu, Q. Zhao, M. H. Li, J. Y. Guan, Y. Zhang, B. Bai, and H. Li, Nature **562**, 548 (2018).
7. R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).
8. A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, and R. Ramanathan, Phys. Rev. A **90**, 032322 (2014).
9. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
10. L. Masanes, S. Pironio, and A. Acín, Nat. Commun. **2**, 238 (2011).
11. S. Wehner, Phys. Rev. A **73**, 022110 (2006).
12. W. Tittel, J. Brendel, and H. Zbinden, Phys. Rev. Lett. **81**, 3563 (1998).
13. J. Barrett, A. Kent, and S. Pironio, Phys. Rev. Lett. **97**, 170409 (2006).
14. N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
15. J. Li, T. J. Liu, S. Wang, C. Jebarathinam, and Q. Wang, Opt. Express **27**, 13559 (2019).
16. O. Andersson, P. Badziąg, I. Dumitru, and A. Cabello, Phys. Rev. A **97**, 012314 (2018).
17. S. Wang, C. X. Liu, J. Li, and Q. Wang, Sci. Rep. **9**, 3854 (2019).
18. M. Xia, J. Li, Y. Hu, W. Sheng, D. Gao, W. Pang, and X. Zheng, Chin. Opt. Lett. **13**, 113001 (2015).
19. Z. Bian, J. Li, H. Qin, X. Zhan, R. Zhang, B. C. Sanders, and P. Xue, Phys. Rev. Lett. **114**, 203602 (2015).
20. X. Han, L. Feng, Y. Li, L. Zhang, J. Song, and Y. Zhang, Chin. Opt. Lett. **17**, 052701 (2019).
21. O. Nieto-Silleras, S. Pironio, and J. Silman, New J. Phys. **16**, 013035 (2014).
22. M. Navascus, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007).
23. P. Wittek, ACM Trans. Math. Software **41**, 21 (2015).
24. A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Phys. Rev. A, **93**, 040102 (2016).